28 April 1997

Viacom International
1515 Broadway, 26th Floor
New York, NY 10036

Attention: Mr. Paul Heimbach, Vice President Engineering

Reference: Merdan's Report of Findings Regarding Our Vulnerability Assessment of a Digital Video Device

Dear Mr. Heimbach:

Please find attached Merdan's Report of Findings. This report provides the results from our security vulnerability assessment of the Matsushita Digital Video Device. We are prepared to discuss the report via teleconference in the event you determine this to be necessary.

If nothing further is received from you by Friday, 2 May 1997, Merdan will return all proprietary data to Matsushita as required by our agreement with that Corporation. If you have any questions, please call either Jim Ludwig or me at [800] 608-6029.

Sincerely,

Linda R. Swilling
Vice President, Finance

Enclosures: Merdan IHD 203-97-118-1U

JWSL:alkw

Attorney Client/Work Product
Outside Counsel's Eyes Only

MERDAN GROUP, INC's.
REPORT OR FINDINGS REGARDING
A DVD VULNERABILITY ASSESSMENT

1.0 INTRODUCTION

The scope of Merdan's this investigation has been limited to the architectural and cryptographic aspects of the Matsushita Electric DVD key management and scrambling schemes. The following restricted access documents were examined:

a. Specifications of DVD Content Scramble System for Key Protection Module Version 0.9, October 1996; Matsushita Electric Industrial Co., Ltd.

b. Specifications of DVD Content Scramble System for Disk Formatter/Scrambler Version 0.9, October 1996; Matsushita Electric Industrial Co., Ltd.

c. Specifications of DVD Content Scramble System for DVD Video Player Version 0.9, October 1996; Matsushita Electric Industrial Co., Ltd.

d. Specifications of DVD Content Scramble System for DVD-ROM Drove Version , October 1996; Matsushita Electric Industrial Co., Ltd.

e. Specifications of DVD Content Scramble System for Decoder Card Version 0.9, October 1996; Matsushita Electric Industrial Co., Ltd.

f. Specifications of DVD Content Scramble System for Descrambler Version 0.9, October 1996; Matsushita Electric Industrial Co., Ltd.

g. Specifications of DVD Content Scramble System for Authenticator on DVD-ROM Drive Version 0.9, October 1996; Matsushita Electric Industrial Co., Ltd.

h. Specifications of DVD Content Scramble System for Authenticator on Decoder Card Version 0.9, October 1996; Matsushita Electric Industrial Co., Ltd.

An overall observation about the difficulty of protecting DVD content versus protecting content for a cable or satellite distribution mechanism of equal strength can be made. Because a pirate has all of the DVD content available before any attempt at cracking is started, the pirates job is inherently easier and potentially requires less technical resources for a DVD scheme than for a cable or satellite distribution mechanism. In a cable or satellite distribution scheme the pirate must store the scrambled content until such time that they are have recovered the keys required to perform descrambling. In a DVD scheme the DVD disk itself provides the storage thus saving the pirate the cost of storing the scrambled content. For some attack, strategies this difference can make these strategies feasible for DVD where they were infeasible for a cable or satellite distribution mechanism. For this reason, to achieve equal strength against a pirate, the cryptographic protection for a DVD scheme needs to be considerably stronger than a cable or satellite scheme or both schemes have to be sufficiently robust to render infeasible all cryptographic pirate attacks.

1.1 ATTACK MODELS

There are a wide range of possible pirate capabilities. To place the strength of a given scheme in perspective, it is appropriate to establish a set of pirate attack models. Each attack model establishes a range of pirate capabilities. Given such ranges of pirate capabilities estimates can made of the likelihood that an attack would in fact be mounted. The arrack models Merdan considered cover an extremely broad range. The following attack models have been found useful in performing security analysis of entertainment content protection schemes:

Happenstance -- In a happenstance attack the pirate discovers some combination of equipment features that defeats or weakens the desired protection. In a happenstance attack the pirate does not add special purpose equipment with the intent of defeating protection or manipulate the equipment outside of it normal operating parameters. An example of a happenstance attack would be to connect a DVD player to a VCR which incorporates Macrovision suppression circuitry.

Casual Hacking -- In a Casual Hacking attack the pirate may add special purpose equipment to defeat or weaken the desired protection. In a Casual Hacking attack the pirate may add a Macrovision suppression device to a standalone DVD player or a VGA to NTSC convertor to a PC based DVD player. The pirate is relatively unsophisticated and does not make any hardware or software modifications inside of the player hardware.

PC Based Medium Sophistication -- In a PC Based Medium Sophistication attack the pirate makes use of a Pentium class PC with an integral or attached DVD drive. The pirate also makes use of utility software that permits them to read and display the DVD at the sector level. The pirate is moderately sophisticated in that they make use of the full range of PC data manipulation tools. The pirates level of sophistication does not extend to use of advanced cryptanalytic methods.

PC Based High Sophistication -- In a PC Based High Sophistication attack the pirate makes use of a Pentium class PC with an integral or attached DVD drive. The pirate also makes use of utility software that permits them to read and display the DVD at the sector level. The pirate is highly sophisticated in that they make use of the full range of PC data manipulation tools and advanced cryptanalytic methods. These methods are discussed only in outline form even in graduate level cryptography textbooks. The limited amount of open literature material available on the topic appears in highly technical academic journals and conference proceedings. The educational level of the pirate is at the graduate level in mathematics, computer science or electrical engineering. The pirate has access to and is familiar with the open literature on cryptanalytic methods.

Low Resource High Sophistication — In a Low Resource High Sophistication attack the pirate makes use of commercially available special purpose hardware and may fabricate their own hardware using high speed programmable logic devices such as Programable Gate Arrays (PGA). The pirate is resource limited in that they will expend less than $5K on special purpose hardware to mount the attack. The educational level of the pirate is at the graduate level in mathematics, computer science or electrical engineering. The pirate has access to and is familiar with the open literature on cryptanalytic methods.

High Resource High Sophistication — In a High Resource High Sophistication attack the pirate makes use of commercially available special purpose hardware and may fabricate their own hardware using high speed programmable logic devices such as Programable PGAs or fabricate Application Specific Integrated Circuits (ASIC). The pirate is not resource limited

in that they will expend $5-500K on special purpose hardware to mount the attack. The educational level of the pirate is at the graduate level in mathematics, computer science or electrical engineering. The pirate has access to and is familiar with the open literature on cryptanalytic methods.

These attack models are intended to cover the entire range of potential pirates from the consumer to criminal enterprises with considerable technical and financial resources. The entire range of pirate attacks encountered in the past is encompassed in these attack models.

2.0 SECURITY ANALYSIS

Merdan's security analysis of the Matsushita DVD scheme is presented in two parts. The first part focuses on the architecture of DVD players and the inherent security limitations engendered by this architecture. The second part focuses on the cryptographic approach employed in the Matsushita DVD scheme.

2.1 ARCHITECTURAL ANALYSIS

Merdan's architectural analysis is based on the inherent architecture of Standalone DVD players and PC based DVD players. It is generic in its nature and does not involve the use of any material received under non-disclosure. The baseline is the technology used to perform MPEG II decoding and the limitations imposed by the high volume commercially available MPEG II decoder Integrated Circuits (IC) used to fabricate consumer DVD players.

2.1.1 Standalone Implementation

The Standalone Implementation has two technical characteristics that render it vulnerable to non cryptographic attacks. The first characteristic is the use of Macrovision to prevent recording of video output. The second characteristic is the presence of an unscrambled, second generation digital, MPEG II stream on the circuit board. Both of these characteristics are well known and are included only to place the cryptographic findings in perspective and to provide a basis for countermeasure identification.

The vulnerability of the Macrovision scheme to add-on devices is well known. In addition, there are reports that some VCR manufacturers have incorporated Macrovision removal circuitry in their commercial product. For this reason, the Macrovision scheme must be considered as vulnerable to a Happenstance attack if the consumer possesses one of the VCRs with inherent Macrovision removal circuitry. The scheme is vulnerability to a Casual Hacking attack if the consumer adds one of the low cost Macrovision suppression add-on devices. It must be recognized that the quality of the recorded content is limited by the VCR and is of analog quality.

The presence of the unscrambled MPEG II stream on the circuit board is a direct result of the architecture of the available MPEG II decoder ICs. At the present time, a full capability MPEG II decoder occupies an entire IC. The semiconductor manufacturers have found it difficult to fit MPEG II on a single IC that is producible at reasonable cost. As a result, the unscrambled MPEG II stream is available on the exposed input pins of the MPEG II decoder. A moderately sophisticated pirate can modify the circuit board to tap this stream and route it to a digital recorder. Once the pirate has recorded the unscrambled MPEG stream they can use this stream to fabricate unscrambled DVDs or to generate analog tapes with the same or better quality than commercial analog video tapes. The level of required resources is relatively low (< $10K) and well within the range of a moderately sophisticated pirate enterprise. It is worth noting that this vulnerability is also present in cable/satellite distribution schemes that use MPEG II and must be

considered as a characteristic of MPEG II rather than DVD.

2.1.2 PC DVD Implementation

The architecture of the PC implementation is inherently much more vulnerable than set top schemes. The present PC based scheme relies on the open PC hardware architecture and functional partitioning between preexisting video hardware and special purpose software running on a high performance processor. By the nature of this architecture there is no place to impose Macrovision in the video stream. The output of the current generation of video cards is component RGB, intended for display by a computer monitor at pixel resolutions of 640 X 480 or greater. Adapters that convert this RGB signal to NTSC are commercially available ($60-180) and are marketed for display of computer output on large screen TVs. It would not be uncommon for a consumer purchasing the PC version to already posses such a converter or to purchase one for the innocent purpose of displaying the output of the PC DVD implementation on their large screen TV. The output of these converters do not presently contain any form of Macrovision and it is very likely that imposition of Macrovision would impede their intended application. If a consumer also has a VCR connected, then recording of the output of the converter must be considered as a natural occurrence. This attack must be considered as Happenstance or at most a Casual Hacking attack.

One of the claimed countermeasures in the PC DVD Implementation is "tamper resistant" software. Similar software based schemes have been in use for copy protection of commercial software for many years. The experience to date has been that all of them have succumbed to moderately sophisticated PC based attacks. The degree of pirate success has been so great that they have fallen into disuse and have been supplanted by hardware based schemes. The technical reason for this is that when a software module is initially loaded into a computer the starting point must be at a clearly defined location in the module. While a sophisticated scheme can be devised that will defeat the unsophisticated pirate, commercially available software debugging tools provide features that allow execution tracing with resolution sufficient to enable reverse engineering of software. In particular, due to the need for high throughput by the descrambler, the executable software will almost certainly be fairly open in structure and straightforward to reverse engineer. It does not appear especially difficult to carry this reverse engineering to the point where the scrambling key could be recovered. By backing up the execution chain, the key management scheme could also be reverse engineered to the extent that the entire key hierarch could be recovered. This class of attack must be considered as PC Based Medium Sophistication since it does not involve cryptanalytic techniques.

2.2 CRYPTOGRAPHIC ANALYSIS

Merdan's cryptographic analysis is presented in three parts. The first part focuses on the key management scheme and its associated cryptography. The second part focuses on the scrambling scheme and its cryptography. The third part addresses the overall scheme, considers attacks on the entire scheme and compares it to schemes based on the Data Encryption Standard. The material in the section is based on proprietary material received under disclosure. For this reason only summary results will be provided. Detailed supporting data would disclose significant aspects of the proprietary information.

2.2.1 Key Management

The management scheme has a straightforward structure that would be obvious to anyone familiar with one or more entertainment content protection schemes. The cryptographic algorithm was clearly designed for efficient software implementation in a modest capability

microprocessor. For this reason, it falls into the Software Encryption Schemes class. Historically, these schemes have nor fared well under cryptanalytic attack. The main reason for this is that the types of operations that lead to cryptographic strength are too inefficient for use in modest microprocessors. These same operations are extremely fast in hardware and consume very small chip areas.

Due to its design, the Key Management scheme can be attacked in stages. The most obvious attack is to perform a bottom up exhaustion attack working upward from the scrambling scheme. This attack would be mounted by using a special purpose hardware attack engine implemented using a small number of PGAs. With an investment of less $10K, for special purpose hardware, and $5K for software tools, an attack engine can be constructed that will take a DVD disk and recover all of the keys used in the protection scheme in less than 6 hours. A more modest version could be constructed for less than $5K, including software tools, that would recover all of the keys for a given DVD disk in 40-80 hours. Once this attack has been successfully mounted for a single DVD, then all other DVDs that use the same master key can be broken with only a PC. It would not be difficult to design a modification of a DVD player that, working in concert with a PC, would use the results of such a break to play any disk in the master key family. The level of sophistication required to mount this attack is dependent on the amount of information available to the pirate. If the restricted Matsushita documents are available, then the design is well within the capabilities of superior B.S.E.E. students and would be within the size range of a class project. Without the restricted documents, relatively sophisticated reverse engineering would be required. Since the software that implements the key management scheme would be present in every player, the Read Only Memories (ROM) would need to be read and reverse engineered. In the worst case, this would require access to a Scanning Electron Microscope. Such equipment has become commonplace in larger University engineering departments and is frequently used by graduate students in semiconductor fabrication classes. There are a number of commercial laboratories that specialize in semiconductor forensics. Even the technicians in such facilities could perform the required ROM readout.

Because of the highly feasible exhaustion attack, an extensive mathematical cryptanalysis of the Key Management scheme was not performed by Merdan. Merdan's preliminary analysis reveals that although the component cryptographic algorithms do not appear to be especially resistant to cryptanalytic attack, the combination of algorithms and their placement in the system design forms a rather effective defense against even the most sophisticated techniques including both differential and linear cryptanalysis. This is because the point of access required by these techniques does not exist in either the Standalone or PC Implementation.

The Key Management scheme must be considered as vulnerable to both Low Resource and High Resource Sophisticated attacks. The design and systematic position of the Key Management Scheme renders it resistant to lesser attacks.

2.2.2 Content Scrambling

The content scrambling scheme is relatively unsophisticated. It is clearly optimized for simplicity and high throughput in a software implementation. It is a member of a family that is thoroughly discussed in several graduate level cryptographic textbooks and research monographs. A special purpose hardware based exhaustion engine can be constructed for an investment of $5-20K that would break any given title in 2-5 hours. This engine can be mass produced, today, in the form of a ASIC at a unit cost of less than $30 (quantity 10,000). A modified player could be constructed that would break any DVD disk in 2-5 hours, the first time, and in real time for subsequent plays. In the next few years advances in semiconductor technology will have the effect of speeding up the process by a factor of 2-3 per year at constant cost. These estimates are

based on knowledge derived from Matsushita restricted material. However, due to its relatively high speed and implementation media, reverse engineering would be somewhat easier than for the Key Management scheme. A few educated guesses, based on graduate course work in cryptography, and some software reverse engineering may be sufficient to support development of the hardware attack without access to restricted data. This attack must be considered as Low Resource Sophisticated for a single unit and high Resource Sophisticated for a mass production unit. Due to the extensive modifications to a DVD player that would be required, it is unlikely that a field modification kit would be offered.

A preliminary mathematical cryptanalysis of the scrambling algorithm was performed by Merdan. Although the analysis was not carried to the point of identifying the details of the attack mechanism, there appears to be a feasible mathematical method for breaking the content scrambling scheme based solely on the algorithm and the underlying structure of the MPEG II stream. If this particular attack or a related attack proved viable then it would be feasible to recover the scrambling key in a few minutes using a PC with a DVD player. Implementation of the results of this attack would require extensive modifications of a player. The level of the modifications are comparable in cost to the hardware attacks described above. As a result the attack falls into the High Resource High Sophistication category.

2.2.3 Overall Scheme

The overall scheme is not especially resistant to sophisticated, hardware based, attack methods. The low resistance is due to inherently weak cryptography. It appears that designers were operating under constraints that limited their options to such an extent that the best they could construct was a cryptographically weak scheme. To place the scheme in perspective it is a factor of 10^4-10^6 weaker than a scheme based on the Data Encryption Standard (DES). DES is also vulnerable to hardware exhaustion attacks but at a considerably greater cost ($50-500K) for comparable break times. Less restrictive constraints could easily result in a scheme that would be cryptographically much more robust.

In the hands of an ordinary consumer, the overall scheme supports delivery of content for the case of compatible combinations of media and player (both standalone and PC based). The determination of the authorized combinations is based on incorporation of the appropriate master key in the player during manufacture. The specifications specifically limit entry of the master key to the manufacturing process. The nature of the protection scheme is such that unauthorized combinations of media and compliant player (both standalone and PC based) will not result in delivery of content. The mechanisms that prevent content delivery in this case are the cryptographic characteristics of the Matsushita DVD protection scheme.

3.0 POTENTIAL REMEDIES

This analysis has revealed that the present DVD protection scheme is vulnerable to a variety of attacks. These vulnerabilities stem from architectural and cryptographic weaknesses. To counter these vulnerabilities several things will be required. First, the exposed MPEG II stream should be eliminated by integrating the descrambler on the same IC with the MPEG II decoder. In order to make this robust, transport of the scrambling key from the Key Management processor to the combined descrambler/decoder will need to be secured. In addition, the scrambling algorithm will need to be replaced with a more robust algorithm. The chip area required to implement an improved scrambling algorithm is less than 10,000 gates. With the move toward .35 micron feature size ICs the additional gates would not appear to be a serious burden.

Resolution of the additional vulnerabilities posed by the PC implementation are problematic. It

is not clear that a pure software solution can be made robust. It may be necessary to use a hardware descrambler/decoder very similar to that used for the enhanced Standalone DVD player. With MPEG hardware appearing even in modest PCs, this may not be as much of a difficulty as it might appear. The next generation video cards could very easily incorporate hardware MPEG II decoders just as many multimedia PCs today incorporate MPEG I decoder hardware. This may also provide a mechanism to impose a variant of Macrovision on the output video.

4.0 CONCLUSIONS

Merdan has reached the following conclusions:

The overall characteristics of the DVD protection scheme are such that in the hands of an ordinary consumer, content will be delivered for authorized combinations of media and player. Content will not be delivered for unauthorized combinations of media and player.

The architectural characteristics of the Standalone Implementation pose significant non cryptographic vulnerabilities.

The overall cryptographic scheme is vulnerable to a low resource sophisticated hardware attack and as result is suitable only for content that is not considered to be worth pirating by a commercial pirate enterprise.

The PC Implementation poses unique vulnerabilities that most likely will need to be resolved by allocating the descrambling and decoding functions to hardware.

In spite of the vulnerabilities found in this analysis the present scheme is superior to unprotected DVD media.

5.0 RECOMMENDATIONS

Merdan proposes the following recommendations:

Deploy the present scheme for content that is not considered to be worth pirating by a commercial pirate enterprise.

Restrict the content to material that will not raise strong official objections from jurisdictions with restrictions against certain types of content.

Investigate alternative architectures for the next generation of players and PC Implementations. These alternatives should integrate the scrambler and MPEG II decoder functions on the same IC.

Give consideration to using a securely authenticated interface to digital interface devices such as digital VCRs. This interface could incorporate a variety of fingerprinting mechanisms.

Further Additions:

Paul

Here is the response of the present system concept to various consumer based attack scenarios. All of these results are based on information from the report. The only thing new here is the form of presentation. As you can see the Standalone Player is relatively resistant to consumer implemented attacks. The consumer attacks based on a Legitimate PC based player or Aftermarket DVD Drive are rather effective, if a pirate enterprise would distribute pure software mechanisms.

A pirate enterprise that is out to make a profit would be stupid to distribute a pure software mechanism since it could be easily pirated. A more profitable approach would be to distribute an mechanism that requires their special hardware. This particular option is the bottom attack mechanism. It should be noted that this mechanism might be advertised over the Internet but would require distribution of hardware via the mails. The VideoCipher II attack was a simplified form of this attack.

Response of DVD Player Configurations to Various Attack Mechanisms

Attack Mechanism	Response of Legitimate Standalone Player	Response of Legitimate PC Based Player	Response of Aftermarket DVD Drive Attached to PC
Consumer manipulation of Standard Controls	Only authorized material will be released	Only authorized material will be released	No material will be released
Consumer modification of legitimate hardware	Required Modifications are far beyond capabilities of ordinary consumer.	Required Modifications are far beyond capabilities of ordinary consumer.	Not Applicable
Consumer modification of legitimate software	Required Modifications are far beyond capabilities of ordinary consumer.	Required Modifications are far beyond capabilities of ordinary consumer.	Not Applicable
Consumer modification of legitimate hardware using kit produced by pirate enterprise	Required Modifications are far beyond capabilities of ordinary consumer.	Required Modifications are far beyond capabilities of ordinary consumer.	Not Applicable

Consumer substitution of software obtained from pirate enterprise, possibly via Internet. Pirate enterprise would have "cracked" all required master keys.	Not feasible	Appears to be entirely feasible. All material scrambled in "cracked" keys would be released.	Entirely feasible. All material scrambled in "cracked" keys would be released.
Consumer substitution of software obtained from pirate enterprise, possibly via Internet. This software would perform key cracking based on a mathematical cryptanalytic method.	Not feasible	Feasible only if pirate enterprise has found mathematical cryptanalytic method. All material scrambled in "cracked" keys would be released.	Feasible only if pirate enterprise has found mathematical cryptanalytic method. All material scrambled in "cracked" keys would be released.
Consumer substitution of software obtained from pirate enterprise, possibly via Internet. This software would perform key cracking using exhaustion methods..	Not feasible	Feasible in theory. In practice the key cracking could take months to years. All material scrambled in "cracked" keys would be released.	Feasible in theory. In practice the key cracking could take months to years. All material scrambled in "cracked" keys would be released.
Consumer installation of hardware/software kit produced by pirate enterprise. This kit includes "cracked" keys stored in protected hardware.	Not feasible	Appears to be entirely feasible. All material scrambled in "cracked" keys would be released.	Entirely feasible. All material scrambled in "cracked" keys would be released.